



**DEPARTMENT OF LABOR AND INDUSTRIAL RELATIONS
COMPUTER SECURITY CONTROLS**

**From The Office Of State Auditor
Claire McCaskill**

*A computer security management plan is needed
to guard against unauthorized access and/or
information loss from disaster.*

**Report No. 2001-41
May 24, 2001
www.auditor.state.mo.us**

PERFORMANCE AUDIT

**DEPARTMENT OF LABOR AND INDUSTRIAL RELATIONS
COMPUTER SECURITY CONTROLS**

TABLE OF CONTENTS

	<u>Page</u>
STATE AUDITOR’S REPORT	1
RESULTS AND RECOMMENDATIONS.....	2
1. The Department of Labor and Industrial Relations Needs to Implement Effective Computer Security Controls and Processes	2
The department has not implemented a risk management program	3
The department lacks an up-to-date disaster recovery plan.....	4
The department did not conduct periodic evaluations to determine the effectiveness of computer security controls.....	4
Employee background screening should be accomplished.....	5
Controls have been implemented to correct some serious security control weaknesses	5
Conclusions.....	6
Recommendations.....	7
2. The Department Needs to Establish a Computer Security Management Program.....	9
A computer security officer would enhance management of risk	9
The department needs to develop comprehensive computer security policies and a security awareness program	9
A recent framework for assessing computer security programs shows the department needs to improve its computer security management program	11
Conclusions.....	11
Recommendations.....	12

**DEPARTMENT OF LABOR AND INDUSTRIAL RELATIONS
COMPUTER SECURITY CONTROLS**

TABLE OF CONTENTS

	<u>Page</u>
APPENDIXES	
I. OBJECTIVE, SCOPE AND METHODOLOGY	13
II. BACKGROUND	14
III. REFERENCES	15
IV. DEPARTMENT OF LABOR AND INDUSTRIAL RELATIONS RESPONSE	16



CLAIRE C. McCASKILL
Missouri State Auditor

Honorable Bob Holden
and
Members of the General Assembly
and
Catherine Leapheart, Director
Department of Labor and Industrial Relations
Jefferson City, Missouri 65102

The State Auditor's Office audited the computer security program at the Department of Labor and Industrial Relations.

The audit objectives were to determine if the Department of Labor and Industrial Relations' computer security program effectively (1) protected computer systems and data against unauthorized access, and (2) ensured recovery of computer processing operations in case of a disaster or other unexpected interruptions.

Audit results disclosed that management needed to improve computer security by developing a risk management process and a new disaster recovery plan, conducting periodic tests and assessments to ensure the effectiveness of existing computer controls, and completing background checks for employees who work in sensitive and critical data processing positions.

Department of Labor and Industrial Relations managers corrected some problems we noted immediately upon being notified and in those instances recommendations were not made in the report. Other issues have been identified and recommendations for corrective action have been made.

Claire McCaskill
State Auditor

February 23, 2001 (fieldwork completion date)

The following auditors participated in the preparation of this report:

Director of Audits: William D. Miller, CIA
Audit Manager: Jeff Thelen, CPA
Audit Staff: John Mollet, CISA
Frank Verslues
Andrea Higgins

RESULTS AND RECOMMENDATIONS

1. The Department of Labor and Industrial Relations Needs to Implement Effective Computer Security Controls and Processes

Audit tests showed that because the Department of Labor and Industrial Relations (the department) does not have a comprehensive computer security management program, it did not implement

- ✓ risk management processes,
- ✓ disaster recovery plans,
- ✓ periodic tests and assessments to ensure implemented controls are effective, and
- ✓ background checks for employees working in sensitive positions.

Without an effective system of computer security controls and processes, the department faces increased risks that mission-essential computer support will not be available, and that confidential data is subject to unauthorized use or destruction.

We attributed the cause for this condition to management not placing priority on the program. However, during the course of our review, department officials took prompt action to correct several of the computer security weaknesses. Accordingly, we are not making recommendations for the weaknesses the department has corrected. We commend the department for taking these immediate steps to decrease the risk of unauthorized use or destruction of financial and confidential data.

Background

The department and its Employment Security and Workers' Compensation Divisions (divisions) rely extensively on information technology to process, pay, and monitor millions of dollars paid annually in unemployment and second injury fund payments, and workers' compensation benefits. The increasing department-wide use and importance of information technology is placing unprecedented demands on security controls over information and the supporting technology.

During fiscal year 2000, the department used its computer systems to process and pay approximately \$300 million in unemployment benefits and approximately \$28 million in second injury fund compensations.¹ Although the department does not directly pay workers' compensation benefits, its computerized files contain over 3 million documents with confidential workers' compensation case data. This data is used to monitor the progress of workers' compensation cases.

According to the National Institute of Standards and Technology, the U.S. Critical Infrastructure Assurance Office, and the U.S. General Accounting Office, effective computer security controls and processes are essential to protect against these unauthorized acts. These nationally and

¹ Computer systems as discussed in this report include hardware (e.g. mainframe computers and servers), software applications, database systems, and telecommunications.

internationally recognized organizations have issued computer security guidelines that show an effective computer security program should include (1) periodic risk and vulnerability assessments, (2) disaster recovery or continuity of operation plans, (3) effective access controls, and (4) periodic evaluations of in-place controls to ensure they are effective.

At the time of our review, the State of Missouri did not have published computer security standards, policies, or guidelines that state agencies were either required or recommended to follow. As a result, we used the above organizations' computer security guidelines as benchmarks to evaluate the adequacy of the department's computer security controls and processes. It should be noted that, as part of its efforts to develop a security architecture for the state, the State of Missouri Information Technology Advisory Board recently prepared a draft set of proposed computer security principles for Missouri state agencies. The Board's proposed security principles were based in part on the National Institute of Standards and Technology computer security publications.

There are no statewide security standards

The department has not implemented a risk management program

Effective security is based on identifying risks and designing security processes and procedures to mitigate them. The first step in establishing effective security is the development of a risk management program.

- ***Risk management*** is the on going process of assessing the risk to computer resources and its data by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.
- ***Risk assessment*** is the process for determining the probability that a particular security threat will exploit system vulnerability.
- ***Threat assessment*** is the process for identifying activities (deliberate or unintentional), such as data input errors, fraud, disgruntled employees, fires, hackers, and viruses, that could harm the system.
- ***Vulnerability assessment*** is the process of identifying flaws or weaknesses that may allow identified threats to harm a computer system or its data.

The department has not initiated or completed any of these essential processes.

According to the Directors of the Divisions of Unemployment Compensation and Workers' Compensation, the loss of computer processing support and computerized data would seriously impact their ability to timely pay unemployment benefits and second injury fund payments, and to monitor workers' compensation cases.

The department has not performed any sensitivity analyses to determine the short- or long-term impact in both monetary and non-monetary terms to their programs if they lost computer-processing support, and if they lost Local Area Network (LAN) support to the State Data Center. These analyses are necessary to ensure that the costs of implementing security controls and disaster recovery plans do not exceed expected losses. Department and division officials have not determined when they will lose the capability to pay weekly benefits after either system is lost. This information is critical to determining when to implement the disaster recovery plan.

Analyses are needed to assess impact if systems fail

The department lacks an up-to-date disaster recovery plan

Disaster recovery or contingency plans should be developed and tested to ensure that critical operations can continue without interruption or can be quickly resumed when unexpected events occur (fires, tornadoes or sabotage). The department's computer center houses two computers and servers connected to the State Data Center. These systems issue an average 6,700 employment benefit payments and an average 72 second injury fund payments each week. Accordingly, it is imperative that the department have a disaster recovery plan, which is updated and tested periodically, to ensure Missouri residents will continue to receive their unemployment or second injury fund payments if the department's computers or LAN are down for an extended period of time.

The department's administrative manual states that in the event of disasters, the department will operate under its disaster recovery information plan and it will not forego processing unemployment insurance claims for more than 5 working days. Although the department has prepared a disaster recovery information plan for the computer center, the plan was prepared in October 1990, and has not been updated. Department officials acknowledged the plan is obsolete and could not be used to reestablish computer processing at an alternate site.

Disaster recovery plan is outdated and obsolete

The department did not conduct periodic evaluations to determine the effectiveness of computer security controls

Although department officials have implemented several computer security controls, they do not conduct any tests or reviews to ensure they are being complied with or working as intended. For example, employees need magnetic key cards to gain access to the computer operations area. Access reports are printed that show the date and time an employee uses his/her card to enter the computer operations area. But, department personnel do not routinely review these reports to identify potential security violations. Our review of the reports for a 7-day period identified numerous incidents where employees had apparently propped open doors for several hours. In one case, a door was left opened for 3 days during a holiday weekend.

Security controls were compromised

Employees are issued user IDs and passwords to authorize access to unemployment and workers' compensation data. Department policy requires an employee's supervisor to notify Information

Systems Section staff to deactivate the employee's user ID and password when employment is terminated. Audit tests showed one section is not following this procedure. New employees are allowed to use the IDs and passwords of departed employees until the new employees receive their IDs and passwords. This practice could result in disgruntled employees using the IDs and passwords to alter or divulge confidential data.

Department managers also do not routinely review computer system reports, which identify what changes have been made to critical functions, such as computer system security values. In fact, managers and staff had not activated a logging system that tracks changes to computer system values. Department officials stated another logging system provides the same information, but acknowledged they were not reviewing these reports. Accordingly, unauthorized changes to critical security controls could go undetected. Department managers do not monitor employee access activity to confidential data to detect failed attempts or unusual patterns of successful access to such information. Routinely monitoring the access activities of employees can help identify significant problems and deter employees from inappropriate and unauthorized activities.

Change tracking system not activated

Additionally, the department's policy does not require division managers to periodically reassess whether employees continue to need access to systems or data, or if current access controls should be changed. As our audit tests showed, periodic evaluations would have identified that several employees did not continue to need the use of powerful user IDs. Also, periodic evaluations would have shown thresholds to automatically log off inactive users were set for an excessive amount of time, which increased the risk of unauthorized access to Departmental data.

Employee background screening should be accomplished

Department managers do not assign different levels of sensitivity to job positions or perform background screening. Sensitivity levels are based on the type and degree of harm, such as disclosure of confidential information, an employee can cause through misuse of computer systems and its data. Sensitivity levels are used to determine if job positions require background screening and if the screening should be done before or after employment. More sensitive positions typically require pre-employment background screening.

Background checks needed for sensitive jobs

Background screening helps determine whether an applicant for employment is suitable for a given position. For example, in positions with access to powerful user IDs, the screening process will attempt to ascertain the applicant's trustworthiness and appropriateness for this position. A senior department official said that background screening should be done for employees working in sensitive positions. For example, the official said he would not want an employee working for him who had been convicted of selling confidential data.

Controls have been implemented to correct some serious security control weaknesses

An essential management objective for all organizations is to protect data from unauthorized access and to prevent intentional or unintentional modification, disclosure, or deletion of

financial or sensitive information. To reduce the risk of unauthorized access and compromise of data, management needs to implement access controls and routinely evaluate the effectiveness of these controls. The department has implemented several management and technical controls to reduce the potential for unauthorized use or destruction of physical assets and data. For example, the department has installed a firewall to control access from outside networks, restricted users' read/write access to sensitive files, required users to change passwords every 30 days, and limited dial-in access to its computers. The department, however, had several significant control weaknesses that posed a risk of inadvertent or deliberate misuse, improper disclosure, or destruction of financial and confidential data.

For example, computers provide a system security control feature to control the amount of time a terminal can remain signed-on without any user activity. Once the inactive threshold is reached, the system automatically logs off the user, requiring the user to undergo a regular sign-on session. The absence of this control feature increases the risk that a terminal may remain logged on and left unattended, thus allowing unauthorized access to the system. The threshold value for the department's Employment Security Division computer was set at "None." This allowed the terminals to remain logged on and left unattended indefinitely. The threshold value for the department's Worker's Compensation Division computer was set at "300." This allowed these terminals to remain logged on and left unattended for 300 minutes, or 5 hours. The length of both of these threshold values increased the risk of unauthorized access to the department's two computer systems.

Unattended computers can lead to access problems

Department officials agreed that both threshold settings were excessive and reduced each setting to 120 minutes or 2 hours. According to department officials, staff often have to leave their computers to attend meetings or to meet with clients; so reducing the settings to less than 2 hours could result in staff losing work if they are automatically logged off the system. Department officials also said department policy requires the use of appropriate security functions or the Windows NT Security Lock which staff activate on their desktop by using computer screen saver passwords. The use of screen saver passwords helps prevent the unauthorized use of staffs' desktop computers when they are away from their computers. It should be noted, however, this policy is not documented in the department's Administrative Manual, and therefore, has not adequately been communicated to all staff.

The department has no established procedures to control access to powerful user identifications (IDs) that can be used to change security values of the department's computer systems. Audit tests showed over 30 staff had access to powerful user IDs to the computer systems. The job functions of many of these staff did not normally require this type of access. Department officials agreed that many of these staff did not require access to this user ID, and reduced access to the powerful user IDs from 30 to 12 staff.

Conclusions

Department officials have not instituted an effective system of computer security controls including, a risk management program, procedures to periodically review computer security controls and employees' data access requirements, and background screening for employees

working in sensitive positions. Accordingly, these officials do not know if the system of computer security controls is adequate to protect computer systems and LAN from unauthorized use or destruction of confidential data. Because the department does not have an updated disaster recovery plan, it has no assurance that payment of unemployment and second injury fund benefits could be continued 5 days after computer operations are lost. The absence of periodic reassessments of computer security controls and employees' system and data access requirements and background screening increases the risk of unauthorized access and use of mission critical data.

With increasing reports of unauthorized access and damage to public and private computer systems and data, the need for risk management programs, disaster recovery plans and effective controls has emerged as critical business imperatives. To meet this need, the National Institute of Standards and Technology has prepared and made available several publications related to computer security. The guidelines contained in these publications are generic and can be used by all public and private organizations.²

Recommendations

We recommend the Director, Department of Labor and Industrial Relations:

- 1.1 Develop a risk management program, that includes (1) asset valuation to determine the near-term and long-term consequences if data are lost or corrupted, and computer and LAN support is lost, (2) threat identification such as, intentional and unintentional errors, disgruntled employees, fire, and natural disaster, (3) vulnerability analysis to determine if current controls could be exploited by identified threats, and (4) design security processes and procedures to mitigate the identified risks that are not currently controlled.
- 1.2 Prepare a disaster recovery plan to ensure the department can continue to process and pay unemployment and second injury fund payments if computer and/or LAN operations are disrupted for an extended period.
- 1.3 Establish a monitoring process to periodically reassess the effectiveness of computer security controls, including computer logging systems and employees' access rights to sensitive systems and data.
- 1.4 Establish a written policy that requires all employees with desktop computers to activate their desktop screen passwords after 5-10 minutes of inactivity.
- 1.5 Assign sensitivity levels to job positions and perform background screening where appropriate.
- 1.6 Follow the procedures and steps in the National Institute of Standards and Technology's Special Publication 800-12, where appropriate, in implementing the above recommendations. This publication and other National Institute of Standards and

²Appendix III page 15, contains a listing of the National Institute of Standards and Technology's publications related to computer security.

Technology computer security related publications are electronically available at <http://csrc.nist.gov>.

Department of Labor and Industrial Relations Responses:

Recommendation 1.1 - The department agrees that a risk management plan is needed and will adhere to the recommendations set forth by the Missouri State Information Technology Advisory Board's Computer Security Principles, upon acceptance, and in conjunction with business area requirements. Finalization of the Missouri State Information Technology Advisory Board's Computer Security Principles is expected by July 1, 2001, and compliance, by all departments, is expected by December 31, 2001.

Recommendation 1.2 - The department agrees that an updated Disaster Recovery Plan is required. Since the original Disaster Recovery Plan was created, the department has had two (2) substantial reorganizations, i.e. transfer of personnel and functions to the Division of Workforce Development, and consolidation with the State Data Center. Now that the reorganizations have been successfully accomplished, it is time to update the Disaster Recovery Plan. The department plans to have the revision implemented by December 31, 2001.

Recommendation 1.3 - The department currently has an access authorization process in place that requires line approval for data/system access. Access Authorization is initiated on the employee's first day on the job and terminated upon divisional acknowledgement of employee departure. Although current system monitoring software logs failed attempts to gain access, the department does not routinely monitor these logs. The monitoring process will be included in the Department's Comprehensive Information Technology Security Plan and will become part of the duties of the Department Information Security Officer referred to in the response to recommendation 2.1.

Recommendation 1.4 - The department agrees with the activation of individual screensavers. This function will activate the Windows NT Security (lock). Employees have been notified to lock their respective workstations if they will be away from their desks for an extended period of time. This directive has been communicated through Inter-Office Memorandums and through line. At the present time it is not official policy. The department is updating procedures contained within the Department's Administrative Manual to include this item as an official policy.

Recommendation 1.5 - The Department agrees that sensitivity levels need to be assigned to job positions and agrees that background screening needs to occur where appropriate. These items will be a part of the Department's Comprehensive Information Technology Security Plan, scheduled for final implementation by July 1, 2001.

Recommendation 1.6 - The department agrees and will adhere to the recommendations set forth by the Missouri State Information Technology Advisory Board's Computer Security Principles, upon acceptance, and in conjunction with business area requirements. Finalization of the Missouri State Information Technology Advisory Board's Computer Security Principles is expected by July 1, 2001, and compliance, by all departments, is expected by December 31, 2001.

2. The Department Needs to Establish a Computer Security Management Program

The department does not have a department-wide computer security management program to ensure computer security receives adequate attention. This is a major contributing cause for the department's lack of risk management processes, disaster recovery plans, and effective access controls. A department-wide security management program should include a computer security officer to function as the central focal point to coordinate computer security, comprehensive security policies, and a continual program of security training and awareness. The department has not made computer security management a priority initiative and has not adequately addressed these objectives.

A computer security officer would enhance management of risk

The department has not clearly designated a central focal point, including a computer security officer, with the responsibility and authority to ensure:

- comprehensive computer security policies
- risk assessments
- disaster recovery plans
- access controls
- security awareness and training programs are implemented

Currently, department officials view the Information Systems section to be the primary organization responsible for computer security. However, as owners and users of several of the department's computer systems, the Divisions of Employment Security and Workers' Compensation are responsible and accountable for certain aspects of the department's computer security program. For example, division officials are responsible for identifying the long- and short-term impacts if they lose computer support and their priority processing requirements in the event of disasters. The divisions also have responsibilities for identifying potential threats such as data input errors and employee sabotage, and reassessing their employees' needs for access to computer systems and data.

Security officer would enhance controls

The department needs to develop comprehensive computer security policies and a security awareness program

According to the National Institute of Standards and Technology, an organization should have a written, up-to-date security policy that covers all major facilities and operations agency-wide. The policy should be approved by key affected parties and cover:

- Security planning
- Risk management
- Review of security controls
- Life-cycle management
- Authorization for processing
- Computer support and operations

- Contingency planning
- Documentation, training, and responses to incidents
- Access controls
- Audit trails

The department's current computer security policies, however, only consist of instructions in its administrative manual that direct employees to (1) access only data that they have been authorized to access, (2) not disclose department data, and (3) not divulge their passwords.

The Information Systems section officials recognized the need for more comprehensive computer security policies when it drafted security policies that addressed 34 specific computer security areas. For example, the draft policy stated all information residing in computers must have system access controls to ensure that it is not improperly accessed, and all users must sign a confidentiality agreement prior to being allowed access to the department's systems. According to Information Systems section officials, the draft policy was reviewed about 2 years ago by senior department officials, but was not formally approved.

The department lacks a computer security awareness and training program

The department's employees play a crucial role in ensuring the security of its computer systems and valuable information resources. According to the U.S. Critical Infrastructure Assurance Office, education, training, and awareness are all necessary to the successful implementation of any computer security program. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. Currently, the department's computer security awareness and training program only consists of a short briefing to new employees on the need to safeguard passwords, and this program was not implemented until November 2000. In addition, the department also does not have an ongoing awareness and training program to periodically reeducate employees on the importance of computer security.

Staff needs
security
awareness
training

The Federal Computer Security Act of 1987 requires federal agencies to provide mandatory periodic training in computer security awareness to all employees who are involved with the management, use, or operation of a computer system within or under the supervision of the agencies. To meet this requirement, the National Institute of Standards and Technology has issued guidelines (Special Publication 800-16) that provide a framework for federal agencies to determine the training needs for different categories of employees involved with the operation and use of computer systems. The department is not a federal agency. However, these guidelines can be used by state agencies to determine the computer security training requirements for their employees and is electronically available at <http://csrc.nist.gov>.

A recent framework for assessing computer security programs shows the department needs to improve its computer security management program

In November 2000, the Federal Chief Information Officers Council (council) in conjunction with the National Institute of Standards and Technology issued a framework for federal agencies to assess the effectiveness of their computer security programs. The document states adequate security of information and the systems that process it are a fundamental management responsibility. Moreover, management must understand the current status of their security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The council's framework security requirements are not new, but are abstracted directly from long-standing requirements found in generally accepted guidance on computer security and privacy. Additionally, the control objectives presented in the framework are generic and can be applied to any organization in the private and public sector.

The computer security assessment framework identifies five levels of computer security program effectiveness, with five being the highest level of security effectiveness. The council stated each federal agency should be at level four striving to get to level five. The Department of Labor and Industrial Relations' computer security program includes some of the elements required to meet up to Level 4 effectiveness but does not include several of the key elements required to meet Level 1 effectiveness. According to the council, a Level 1 security program consists of a formally documented program that establishes a continuing, agency-wide cycle of assessing risk, implements effective security policies including training, and promotes monitoring for program effectiveness. As discussed in this report, the department has not developed a formally documented computer security program that contains the elements suggested by the council.

There are standards for security available

As noted in *appendix I, page 13*, of this report, our audit did not include all computer security controls. Therefore, the department may have additional computer security control weaknesses, which could result in unauthorized access to the department's systems and data. At the completion of our audit, the National Institute of Standards and Technology issued a self-assessment guide that builds on the November 2000 framework developed for the council. The guide includes an extensive questionnaire containing several computer security control objectives, which we did not test. This guide is designed for use by all levels of management and by those individuals responsible for computer security at the system level and organization level, and is electronically available at <http://csrc.nist.gov>.

Conclusions

The absence of a departmental security management program, which includes central responsibility, comprehensive security policies, and employee security awareness programs has resulted in a security program that lacks several critical processes. These processes include (1) an ongoing risk management program, (2) disaster recovery plans, (3) routine monitoring to ensure security program effectiveness, and (4) background screening for employees working in sensitive positions.

Recommendations

We recommend the Director, Department of Labor and Industrial Relations:

- 2.1 Assign overall responsibility and authority for the department's computer security program to an appropriate senior official, and designate a department computer security officer.
- 2.2 Develop comprehensive computer security policies that include such elements as security planning, risk management, periodic reviews of security controls, personnel background screening, contingency planning, training, access controls, and audit trails.
- 2.3 Use the National Institute of Standards and Technology computer security self-assessment guide to evaluate the effectiveness of its computer security program and make improvements where needed.
- 2.4 Establish a security awareness and training program based on National Institute of Standards and Technology guidelines as appropriate.

Department of Labor and Industrial Relations Responses:

Recommendation 2.1 - Although the State of Missouri does not currently have a position description listed for an Information Security Officer (ISO), the department is researching, and drafting the Department Information Security Officer (DISO) position description for submission to the Office of Administration, Division of Personnel. Upon acceptance by the Office of Administration, Division of Personnel, the department will request appropriate funding for the establishment of this position. Prior to establishment of the position, the department plans to assign the specific duties and responsibilities to an appropriate staff member. Estimated date of this assignment will be prior to August 15, 2001.

Recommendation 2.2 - The department is in the process of developing a comprehensive computer security policy. The policy is scheduled for implementation July 1, 2001. This policy will include security planning, risk management, periodic reviews of security controls, personnel background screening, contingency planning, training, access controls, and audit trails.

Recommendation 2.3 - The department will utilize the recommended computer security self-assessment guide to evaluate the effectiveness of its computer security program.

Recommendation 2.4 - The department will establish a security awareness and training program based on National Institute of Standards and Technology guidelines as appropriate. Estimated implementation will be with the completion of the department's comprehensive Information Technology Security Plan on July 1, 2001.

OBJECTIVE, SCOPE AND METHODOLOGY

Objectives

Our objectives were to determine if the Department of Labor and Industrial Relations' computer security program effectively (1) protects computer systems and data against unauthorized access, and (2) ensures recovery of computer processing operations in case of a disaster or other unexpected interruptions.

Scope and Methodology

Specifically, we evaluated the department's computer security program that is intended to:

- Protect data and application programs from physical and logical unauthorized access.
- Prevent the introduction of unauthorized changes to application and system software.
- Provide segregation of duties involving application programming, system programming, computer operations, information security, and quality assurance.
- Ensure recovery of computer processing operations in case of a disaster or other unexpected interruptions.
- Ensure adequate computer security program management.

To evaluate these controls, we identified and reviewed the department's and divisions' policies and procedures, interviewed responsible officials, and conducted tests and observations of controls to determine if system controls were in place, adequately designed, and operating effectively. Since the State of Missouri has not established statutes and regulations that prescribe standards for computer system operating controls, we based our audit on the U. S. General Accounting Office's Federal Information System Controls Audit Manual. This manual provides guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data. In addition to the manual, we used generally accepted computer security program principles and guidelines published by the National Institute of Standards and Technology, and the U.S. Critical Infrastructure Assurance Office.

We conducted our review from January through March 2001. The audit was made in accordance with generally accepted government auditing standards and included such tests of the procedures and records as were deemed appropriate. Because the objective of our review was to assess the overall effectiveness of the department's computer general controls, we did not fully evaluate all computer controls.

APPENDIX II

BACKGROUND

The Omnibus State Reorganization Act of 1974 established the current Department of Labor and Industrial Relations (the department). The department is responsible for administering (1) the Unemployment Insurance program that provides an income contribution for workers to offset the loss of employment due to layoff, and (2) the Workers' Compensation program that provides an income contribution for workers to offset the loss of a job because of injury.

Unemployment insurance programs in Missouri began under federal guidelines in the 1930s. The department's Division of Employment Security is responsible for the day-to-day operations of Missouri's unemployment insurance program. These responsibilities include collecting unemployment contributions paid by Missouri employers and paying unemployment benefits to individuals who are eligible under the law. In fiscal years 1999 and 2000, the department paid \$399 million and \$299.8 million, respectively, to qualified claimants for unemployment compensation.

The department's Division of Workers' Compensation has been administering Missouri's workers' compensation laws since 1926. This responsibility includes monitoring workers' compensation cases and payments as well as determining the payment of second injury fund benefits. In fiscal year 2000, the Division of Workers' Compensation paid \$27.6 million in second injury fund benefits.

The department's Information Systems section provides data processing support to the Divisions of Employment Security and Workers' Compensation. The Information Systems section operates the department's two computer systems and Local Area Network (LAN), which are used by the Employment Security Division to support the payment of weekly unemployment benefits. The Workers' Compensation Division uses the two computer systems and LAN to monitor workers' compensation cases and payments and to directly pay second injury fund payments.

REFERENCES

National Bureau of Standards

Guidelines For Automatic Data Processing Physical Security and Risk Management: Federal Information Processing Standards Publication 31. June 1974. <http://csrc.nist.gov>.

Guidelines For Security Of Computer Applications: Federal Information Processing Standards Publication 73. June 30, 1980. <http://csrc.nist.gov>.

National Institute of Standards and Technology

Keeping Your Site Comfortably Secure: An Introduction to Internet Firewall. Special Publication 800-10. December 1994. <http://csrc.nist.gov>.

An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. October 1995. <http://csrc.nist.gov>.

Generally Accepted Principles and Practices for Securing Information Technology Systems. Special Publication 800-14. September 1996. <http://csrc.nist.gov>.

Information Technology Security Training Requirements: A Role And Performance Base Model. Special Publication 800-18. April 1998. <http://csrc.nist.gov>.

Guide For Developing Security Plans For Information Technology Systems. Special Publication 800-18. December 1998. <http://csrc.nist.gov>.

Self-Assessment Guide For Information Technology Systems. Special Publication 800-XX. Draft - March 9, 2001. <http://csrc.nist.gov>.

Critical Infrastructure Assurance Office

Practices For Securing Critical Information Assets. January, 2000. www.ciao.gov

Defending America's Cyberspace: National Plan For Information Systems Protection. Version 1.0. 2000. www.ciao.gov

Federal Chief Information Officers Council

Federal Information Technology Security Assessment Framework. November 28, 2000. www.cio.gov

U.S. General Accounting Office

Federal Information Systems Control Audit Manual: GAO/AIMD-12.19.6. January 1999. www.gao.gov

State of Missouri, Information Technology Advisory Board

A Proposed Set Of Information Security Principles For Missouri State Government. Draft – December 5, 2000.



MISSOURI DEPARTMENT OF LABOR AND INDUSTRIAL RELATIONS

POST OFFICE BOX 504
JEFFERSON CITY, MISSOURI 65102-0504
PHONE: (573) 751-9691 FAX: (573) 751-4135

APPENDIX IV

CATHERINE B. LEAPHEART
DEPARTMENT DIRECTOR

THOMAS J. PFEIFFER
DEPUTY DIRECTOR

April 17, 2001

APR 18 2001

Mr. Jeff Thelen, CPA
Audit Manager
Missouri State Auditor's Office
Truman State Office Building, Room 880
Jefferson City, MO 65101

Dear Mr. Thelen:

The Missouri Department of Labor and Industrial Relations, in response to the "Draft" Computer Security Audit, provides the following acknowledgements:

- 1) Draft letter to "Honorable Bob Holden and Members of the General Assembly" should be changed to indicate the "updating of the Department Disaster Recovery Plan" and not the initial development of said plan. This is in direct relation to page 3, paragraph 3 of the report.
- 2) Page 2, paragraph 3 – It should be stated that these benchmarks, although appropriate in most cases, have not been adopted by the State of Missouri at present. Although specific standards are not available for the Department's adherence, the Department has initiated numerous procedures for the control and access of data.
- 3) Page 3, paragraph 4 – It should be noted that prior to notification of this audit, the Department had initiated research into the acquisition of an Intrusion Detection System. A copy of the preliminary research was provided to the audit team for their review. Currently, the Department is preparing a final report for the acquisition, and implementation, of the proposed Intrusion Detection System.
- 4) Page 4, paragraph 2 – It should be noted that the wording "Department officials also said Department policy requires staff to activate their desktop computer screen saver passwords" is incorrect. Department policy, Sub-section H of Section B05-72090 of the Department's Administrative Manual, indicates that the "Windows NT Security (lock), or similar functions should be used when appropriate".
- 5) Page 4, paragraph 5 – It should be noted that the incident of door ajar was due to an improperly closing door and has since been remedied with the installation of magnetic locking mechanisms during access control modifications. Information Systems' management has initiated procedures requiring that access security control be strictly adhered to.

APPENDIX IV

Mr. Jeff Thelen, CPA
April 17, 2001
Page 2

- 6) Page 9, paragraph 3 – It should be noted that the Missouri Department of Labor and Industrial Relations is not a federal agency, but will adhere to the recommendations set forth by the Missouri State Information Technology Advisory Board's Computer Security Principles, upon acceptance, and in conjunction with business area requirements.
- 7) Page 10, paragraph 2 – It should be noted that discussion between the Senior Auditor and the Department's Chief Information Officer, indicated that although the Department's computer security program did not include key elements required to meet Level 1 effectiveness, the computer security program did meet several key elements required to meet up to and including Level 4 effectiveness.
- 8) It should be noted that multiple references listed within Appendix III have been established recently and although they apply, they require substantial time for implementation. The standards set forth in these references will be adhered to once adopted by the Missouri State Information Technology Advisory Board.

Recommendations.

- 1.1 The Department agrees that a risk management plan is needed and will adhere to the recommendations set forth by the Missouri State Information Technology Advisory Board's Computer Security Principles, upon acceptance, and in conjunction with business area requirements. Finalization of the Missouri State Information Technology Advisory Board's Computer Security Principles is expected by July 1, 2001 and compliance, by all Departments, is expected by December 31, 2001.
- 1.2 The Department agrees that an updated Disaster Recovery Plan is required. Since the original Disaster Recovery Plan was created, the Department has had two (2) substantial reorganizations, i.e. transfer of personnel and functions to the Division of Workforce Development, and consolidation with the State Data Center. Now that the reorganizations have been successfully accomplished, it is time to update the Disaster Recovery Plan. The Department plans to have the revision implemented by December 31, 2001.
- 1.3 The Department currently has an access authorization process in place that requires line approval for data/system access. Access Authorization is initiated on the employee's first day on the job and terminated upon Divisional acknowledgement of employee departure. Although current system monitoring software logs failed attempts to gain access, the Department does not routinely monitor these logs. The monitoring process will be included in the Department's Comprehensive Information

Mr. Jeff Thelen, CPA
April 17, 2001
Page 3

Technology Security Plan and will become part of the duties of the Department Information Security Officer referred to in the response to recommendation 2.1.

- .4 The Department agrees with the activation of individual screensavers. This function will activate the Windows NT Security (lock). Employees have been notified to lock their respective workstations if they will be away from their desks for an extended period of time. This directive has been communicated through Inter-Office Memorandums and through line. At the present time it is not official policy. The Department is updating procedures contained within the Department's Administrative Manual to include this item as an official policy.
- 1.5 The Department agrees that sensitivity levels need to be assigned to job positions and agrees that background screening needs to occur where appropriate. These items will be a part of the Department's Comprehensive Information Technology Security Plan, scheduled for final implementation by July 1, 2001.
- 1.6 The Department agrees and will adhere to the recommendations set forth by the Missouri State Information Technology Advisory Board's Computer Security Principles, upon acceptance, and in conjunction with business area requirements. Finalization of the Missouri State Information Technology Advisory Board's Computer Security Principles is expected by July 1, 2001 and compliance, by all Departments, is expected by December 31, 2001.

Recommendations.

- 2.1 Although the State of Missouri does not currently have a position description listed for an Information Security Officer (ISO), the Department is researching, and drafting the Department Information Security Officer (DISO) position description for submission to the Office of Administration, Division of Personnel. Upon acceptance by the Office of Administration, Division of Personnel, the Department will request appropriate funding for the establishment of this position. Prior to establishment of the position, the Department plans to assign the specific duties and responsibilities to an appropriate staff member. Estimated date of this assignment will be prior to August 15, 2001.
- 2.2 The department is in the process of developing a comprehensive computer security policy. The policy is scheduled for implementation July 1, 2001. This policy will include security planning, risk management, periodic reviews of security controls, personnel background screening, contingency planning, training, access controls and audit trails.


Mr. Jeff Thelen, CPA
April 17, 2001
Page 4

The Department will utilize the recommended computer security self-assessment guide to evaluate the effectiveness of its computer security program.

The Department will establish a security awareness and training program based on National Institute of Standards and Technology guidelines as appropriate. Estimated implementation will be with the completion of the Department's comprehensive Information Technology Security Plan on July 1, 2001.

If you have any questions or need additional clarification, do not hesitate to contact me at 751-9691.

Sincerely,



Thomas J. Pfeiffer
Deputy Director